UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/944,788	08/31/2001	Alfonso De Jesus Valdes	10454-022001/P-4190-4	1821

52197 7590 09/11/2009

Wall & Tong, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SHREWSBURY, NJ 07702

EXAMINER	
SHERR, CRISTINA O	

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
09/11/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/944,788	VALDES ET AL.	
	Examiner	Art Unit	
	CRISTINA SHERR	3685	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05/07/09*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) *3-6,9-12,15-30* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,7,8,13 and 14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

SUPPLEMENTAL DETAILED ACTION

1. The Non-Final Rejection issued on August 31, 2009 is hereby withdrawn, and the following issued in its place.

2. This Office Action is in response to Applicant's Amendment filed May 7, 2009.

Election/Restrictions

3. Applicant's election without traverse of claims 1, 2, 7, 8, 13, and 14 (invention I) in the reply filed on May 7, 2009 is acknowledged. Accordingly, claims 1-30 are pending in this case and claims 1, 2, 7, 8, 13, and 14 are currently under examination. Claims 1, 7, and 13 are currently amended.

Response to Arguments

4. Applicant's arguments, see Remarks, filed November 24, 2008, with respect to the section 112 rejection of claims 1, 2, 7, 8, 13, and 14, as currently amended, have been fully considered and are persuasive. The section 112 rejection of 1, 2, 7, 8, 13, and 14 has been withdrawn.

5. Applicant's arguments filed November 24, 2008, regarding the section 103 rejections of claims 1, 2, 7, 8, 13, and 14, as currently amended, have been fully considered but they are not persuasive.

6. Applicant argues, regarding claims 1, 7, and 13, that nothing in the cited reference discloses, teaches or suggests "comparison of an alert (indicating an attack or anomalous incident) - or more specifically, the comparison of features of the alert - to the features of existing alert classes, in order to classify the alert".

7. Examiner respectfully disagrees and directs attention to Nine as follows. In Nine, "Upon receipt of the ticket, receiver process 250 parses the ticket and uses the information in the ticket to query accounting engine 248 for information on where to place the pending ticket (step 538)." (col 8 ln 38-41). In parsing the ticket, the receiver is taking features of the alert then comparing them to other alerts and classifying the alert, which is deciding where to place the pending ticket. In other words, the pending ticket gets placed with similar pending tickets, which are those in the same class. The class is decided by comparing the features of the ticket to features of other tickets. Further, it follows that if the features obtained in parsing the ticket or alert are very different from all other alerts, then the instant alert cannot be placed with others, and will eventually form its own class.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

10. Claims 1-2, 7-8, and 13-14 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter

11. In this case, claims 1-2 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Based on Supreme Court precedent (See also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981); *Parker v. Flook*, 437

U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972); *Cochrane v. Deener*, 94 U.S. 780, 787-88 (1876)) and recent Federal Circuit decisions, a §101 process must (1) be tied to another statutory class (such as a particular apparatus) or (2) transform underlying subject matter (such as an article or materials) to a different state or thing. In addition, the tie to a particular apparatus, for example, cannot be mere extra-solution activity. See *In re Bilski*, 88 USPQ2d 1385 (Fed. Cir. 2008). To meet prong (1), the method step should positively recite the other statutory class (the thing or product) to which it is tied. This may be accomplished by having the claim positively recite the machine that accomplishes the method steps. Alternatively or to meet prong (2), the method step should positively recite identifying the material that is being changed to a different state or positively recite the subject matter that is being transformed.

12. Specifically, regarding claim 1, the device or machine represents mere extra-solution activity, as part of a preamble. The various steps in claim 1 can be reasonably interpreted as being performed by a person alerting another person via a shout, for example, or via mental steps in comparing one alert with another. Further, no material is being changed to a different state. For these reasons, independent claim 1 and its dependent claim 2 are rejected under section 101.

13. Under the broadest reasonable interpretation standard, claims 7-8 and 13-14 recite a computer program only. "Computer programs claimed as computer listings per se, *i.e.*, the descriptions or expressions of the programs, are not physical 'things.' They are neither computer components nor statutory processes, as they are not 'acts' being

performed." MPEP §2106.01 I. Because the claims recite only abstractions that are neither "things" nor "acts," the claims are not within one of the four statutory classes of invention.[1] Because the claims are not within one of the four statutory classes of invention, the claims are rejected under 35 U.S.C. §101.

14. In this case, independent claim 7 recites a "computer readable medium containing an executable program . . ." The claim recites neither computer components nor statutory processes, as they are not "acts" MPEP §2106.01 I. Because the claim recites only abstractions that are neither "things" nor "acts," the claim(s) are not within one of the four statutory classes of invention. Because independent claim 7 is not within one of the four statutory classes of invention, independent claim 7 and its dependent claim 8 are rejected under 35 U.S.C. §101.

15. In this case, claim 13 recites means for receiving, updating, identifying, updating, comparing, and associating, where, according to the broadest reasonable interpretation of the claims, such means are interpreted as software only. Thus, the claim recites neither computer components nor statutory processes, as they are not "acts" MPEP §2106.01 I. Because the claim recites only abstractions that are neither "things" nor "acts," the claim(s) are not within one of the four statutory classes of invention. Because independent claim 13 is not within one of the four statutory classes of invention, independent claim 13 and its dependent claim 14 are rejected under 35 U.S.C. §101.

---

[1] 35 U.S.C. §101 defines four categories of inventions that Congress deemed to be the appropriate subject matter of a patent; namely, processes, machines, manufactures and compositions of matter. The latter three categories define "things" (or products) while the first category defines "actions" (*i.e.*, inventions that consist of a series of steps or acts to be performed).

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

17. Claims 1, 2, 7, 8, 13, and 14 are rejected under 35 U.S.C. 102(a) as being anticipated by Nine et al (US 6,560,611).

18. Regarding claims 1, 7, and 13 –

19. Nine discloses in an intrusion detection system (abs, col 2 ln 65-67) that includes a plurality of sensors (e.g. col 3 ln 1-5) that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features (col 4 ln 52-55), the method comprising the steps of:

(a) receiving a new alert (called "message" at col 3 ln 25-30 or "ticket" at col 3 ln 15-20, col 5 ln 32-34, col 7 ln 47-50, col 7 ln 63-col 8 ln 9);

(b) identifying a set of similar features shared by the new alert and one or more existing alert classes (e.g. col 3 ln 12-20, col 8 ln 35-42);

(c) updating a threshold similarity requirement for one or more features (e.g. col 5 ln 50-col 6 ln 10, col 9 ln 22-40);

(d) updating a similarity expectation for one or more features (e.g. col 5 ln 50-col 6 ln 10, col 9 ln 30-35);

(e) comparing the new alert with one or more alert classes, and either:

(f 1) associating the new alert with the existing alert class that the new alert most closely matches (col 7 ln 22-46, col 5 ln 32-37, col 8 ln 35-42); or

(f 2) defining a new alert class that is associated with the new alert (col 9 ln 5-40).

20. Regarding claims 2, 8, and 14 –

21. Nine discloses the method of claim 1 further comprising the step (a) of passing each existing alert class through a transition model to generate a new prior belief state for each alert class (e.g. col 5 ln 60- col 6 ln 10, col 9 ln 22-40).

22. As above, although Nine discloses messages rather than "alerts", the said messages are the functional equivalents of alerts, where generally, the disclosure of Nine may be adapted by one of ordinary skill in the art to obtain the instant application.

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CRISTINA SHERR whose telephone number is (571)272-6711. The examiner can normally be reached on 8:30-5:00 Monday through Friday.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Calvin L. Hewitt, II can be reached on (571)272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

25. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CRISTINA OWEN SHERR
Examiner
Art Unit 3685

/Calvin L Hewitt II/
Supervisory Patent Examiner, Art Unit 3685